

Notice of Allowability

Application No.

10/000,396

Examiner

Ronald Baum

Applicant(s)

COPELAND, JOHN A.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/28/06.
2. ☒ The allowed claim(s) is/are 1-37.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

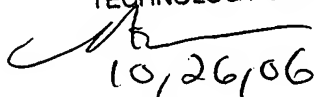
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 20061024.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


10,26,06

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John R. Harris, Reg. No. 30,388 on 10/24/2006.

1. Replace claim 37 with the following (shown *marked up* here, followed by *clean version*):

37. The method of claim 6, wherein the predetermined concern index characteristic comprises one or more of the following characteristics:

potential TCP probe,

potential UDP probe,

half-open attack,

TCP stealth port scan,

UDP stealth port scan,

bad flags,

short UDP,

address scan,

port scan.

Clean claim version:

37. The method of claim 6, wherein the predetermined concern index characteristic comprises one or more of the following characteristics:

potential TCP probe,
potential UDP probe,
half-open attack,
TCP stealth port scan,
UDP stealth port scan,
bad flags,
short UDP,
address scan,
port scan.

Examiner's Statement of Reasons for Allowance

2. Claims 1-37 are allowed over prior art.
3. This action is in reply to applicant's correspondence of 26 August 2006.
4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

5. As per claims 1,6,8,10,11 and 12 generally, prior art of record, Shipley, U.S. Patent 6,119,236, fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 8/28/2006 to office action of 5/23/2006.

Specifically, (as per claim 1, for example) prior art dealing with network traffic anomaly/misuse detection/analysis via various signature capture/learning methodologies, is generally known to exist per se, (i.e., MAHONEY, M., "Network Traffic Anomaly Detection Based on Packet Bytes", ACM, 2003, FI. Institute of Technology, entire document, <http://www.cs.fit.edu/~mmahoney/paper6.pdf>). Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the determination of suspicious activity (and the issuance thereof of a subsequent notification/alarm) as a function of a threshold exceeded for an accumulated flow count that is itself a function of the packet count *and* service associated with the collected/predetermined flow), at the *time of the invention*; serving to patently distinguish the invention from said prior art (as contrasted against simple packet signature matching in the prior art);

"1. A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious activity, comprising the steps of:

monitoring packet headers of packets exchanged between

two hosts on the data communication network;

based on the packet headers, determining the existence of a client/server (C/S) flow as corresponding to

*a predetermined plurality of packets exchanged between the two hosts
that relate to a single service and
is characterized by a predetermined C/S flow characteristic;
assigning a concern index value to a determined C/S flow based upon
a predetermined concern index characteristic of the C/S flow;
maintaining an accumulated concern index comprising
concern index values for one or more
determined C/S flows associated with a host; and
issuing an alarm signal in the event that
the accumulated concern index for a host exceeds an alarm threshold value.”*

6. Dependent claims 2-5,7,9,13-37 are allowable by virtue of their dependencies.

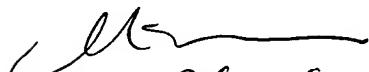
Conclusion

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


10/26/06

Ronald Baum

Patent Examiner

